



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/767,529	01/29/2004	Brian Bernard McKeon		5527

7590
BRIAN MCKEON
11A BOORALIE RD.
TERREY HILLS, NSW, 2084
AUSTRALIA

EXAMINER

TABOR, AMARE F

ART UNIT	PAPER NUMBER
----------	--------------

2434

MAIL DATE	DELIVERY MODE
-----------	---------------

05/09/2011

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/767,529

Applicant(s)

MCKEON, BRIAN BERNARD

Examiner

AMARE TABOR

Art Unit

2434

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 December 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3,4 and 6-8 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3,4 and 6-8 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsman's Patent Drawing Review (PTO-940)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This is in response to REMARKS filed on 12/01/2008.
2. Claims 1, 3, 4 and 6-8 are pending.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 3, 4 and 6-8 are rejected under 35 U.S.C. 102(e) as being anticipated by
“Aull” (US 7,047,409 B1)

As per Claim 1, Aull teaches,

A computer system for a computer device providing cryptographic tickets to be transmitted to one or more trusted modules [see **CERTIFICATE AUTHORITY 110 & TOKEN 130** in FIGS.1-3], allowing intended modules to issue a set number of public-key certificates [see for example, col.3, lines 37-48, “... *an automated registration arrangement... can be accessed only via the associated pedigree certificate, ... if a user accesses one of the special Registration Web pages, the user must be employing the special hardware of the corresponding category since only that category of hardware possesses the requisite pedigree certificate and associated private key. Thus, the user*”]

can be issued a digital certificate having a level of trust commensurate with the pedigree certificate of the special hardware of the user". See also FIG.2; and for example, col.5, line 61 to col.6, line 23].

As per Claims 3, 6 and 8, Aull teaches,

A computer system based on the method of claim 1 where the trusted module is a hardware token such as a USB token or a smartcard [see for example, col.3, lines 31-36, "*In accordance with the present invention, specific categories of hardware, such as **smart cards or USB (Universal Serial Bus) tokens**, are pre-loaded with a pedigree certificate and associated private key designating the hardware type, one pedigree certificate being designed for each category of hardware*".]

As per Claim 4, Aull teaches,

A computer system based on claim 1, where the cryptographic ticket is a public-key or private-key certificate [see FIG.2; and for example, col.6, lines 4-23, "*In step 1 of FIG. 2, ... In step 2, ... In step 3, a **public/private key pair is generated** by either the local registration authority 250 software or the registration authority 112 software, depending on the products chosen and depending on how they've been configured. The public key is sent to the certificate authority 110 to be signed, thereby generating a "certificate". In step 4...*"]

As per Claim 7, Aull teaches,

A computer system based on claim 1, where the set number of certificates that can be issued is determined by information within the provided cryptographic ticket [see for example, abstract, “A *method of automatically tracking a certificate pedigree is provided, in which a new user is provided with a piece of hardware containing a **predetermined pedigree certificate stored therein**, the predetermined pedigree certificate having a level of trust bearing a relationship to a category of hardware of which the provided piece of hardware is a member. An automated registration arrangement ...*”]

Response to Arguments

4. Applicant's arguments filed on 08/27/2008 and 12/01/2008 have been fully considered but they are not persuasive.

Applicant argues that “...the invention uses hardware tokens, not as a certificate and key store for end-users but as an intermediate Certificate Authority that can be securely regulated by the parent CA...”

Examiner respectfully disagrees and notes that, independent claim 1 recites, “A computer system for a computer device providing cryptographic tickets to be transmitted to one or more **trusted modules**, allowing intended modules to issue a set number of public-key certificates”. With broadest but reasonable interpretation, a “trusted module” is any trusted entity that issues PKI certificates after receiving cryptographic tickets. For example, Aull teaches (Abstract and FIG.1) an automated registration arrangement that

stores certificates issued by a certificate authority. Users can access the registration arrangement with a piece of hardware. The registration arrangement, acting as an intermediate CA between the CA and users, provides (or issues) certificates to new users. Furthermore, Aull teaches (see FIG.2) "registration authority" (e.g. 250 in FIG.2) generating a public/private key pair then sending the public key (claimed "cryptographic ticket") to Certificate Authority 110 to be signed, thereby a certificate is generated (i.e., "PKI certificates" are issued). In this arrangement, the registration authority provides the public keys as crypto-tickets to the CA (acting as an intermediate CA), and the CA issues public key certificates.

In response to applicant's argument that the references fail to show certain features of applicant's invention (as claimed in independent claim 1), it is noted that the features upon which applicant relies (i.e., "Hardware Token for sub-issuance CA") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicant's arguments are unpersuasive; and the rejection is respectfully maintained, and the action is made final.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **AMARE TABOR** whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **KAMBIZ ZAND** can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Amare Tabor/
Examiner, Art Unit 2434

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434